Traccia:

La figura nella slide successiva mostra un estratto del codice di un malware.
Identificate:

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una **descrizione** per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la **persistenza** sul sistema operativo
4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Basandoci sulle chiamate di funzione utilizzate, sembra che questo malware sia progettato per agire come un "keylogger", un tipo di malware che registra e trasmette le attività della tastiera dell'utente ad un'entità remota.

Ecco le descrizioni delle chiamate di funzione principali utilizzate:

- **SetWindowsHook()**: Questa funzione imposta un hook di Windows, consentendo al malware di intercettare eventi del mouse. Nel contesto del malware, è probabile che sia utilizzata per registrare l'input del mouse, oltre all'input della tastiera, se il malware ha funzionalità di keylogging.
- **CopyFile()**: Questa funzione viene utilizzata per copiare un file specificato in un'altra posizione. Nel contesto del malware, è utilizzata per copiare il file del malware stesso in una cartella di avvio del sistema operativo, presumibilmente per ottenere persistenza.

Metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo:

Il malware utilizza la funzione **CopyFile()** per copiare se stesso in una cartella di avvio del sistema operativo. Questa è una tecnica comune utilizzata dai malware per garantire che vengano eseguiti automaticamente ogni volta che il sistema operativo viene avviato. In questo caso, sembra che il malware stia cercando di ottenere persistenza copiandosi nella cartella di avvio del sistema, in modo da essere eseguito all'avvio successivo del sistema operativo.